DISKCRYPT MOBILE

DCM300

MANUALE D'USO

This page has been left blank intentionally

ST Electronics (Info-Security)

ST Electronics
A company of ST Engineering

DiskCrypt® *Mobile*

MANUALE D'USO

G-P6019-TM001
(ISSUE B)

Issue Date: Mar 2010

Copyright
© 2009 ST Electronics (Info-Security) Pte Ltd. Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotto, riscritto,utilizzato da terze parti in ogni forma senza permesso scritto di ST Electronics (Info-Security) Pte Ltd.

Trademarks
Il logo DigiSAFE e DiskCrypt sono marchi registrati della ST Electronics (Info Security) Pte Ltd in Singapore e altri Paesi. Il logo DigiSAFE è marchio registrato in U.S. Patent e Trademark office. Tutti gli altri marchi registrati sono di proprietà dei rispettivi proprietari

2010.03.23 Version 1.2

ST Electronics (Info-Security) Pte Ltd
ST Electronics Jurong East Building
100 Jurong East Street 21
Singapore 609602
Tel: (65) 6568 7118
Fax: (65) 6568 7226
Email: info@digisafe.com
Website: www.digisafe.com

Importato da:
ECore S.r.l.
Piazzale Cadorna 6
20123 Milano
Website: www.ecore.it
Email: info@ecore.it

This page has been left blank intentionally

Disclaimer

Il DigiSAFE DiskCrypt *Mobil*e DCM300 è conforme alle specifiche standard SATA hard disk Drive e USB 1.1/2.0 e Firewire 400/800.

ST Electronics (Info Security) non assume alcuna responsabilità per eventuali perdite di Dati o inabilità del DiskCrypt Mobile per operare con macchine non conformi alle suddette Specifiche operative. ST Electronics (Info Security) non risponde di software che non sia compatibile.

Grazie per aver acquistato DiskCrypt *Mobile*.

Contenuto

1. Informazioni sul manuale 1

2. Introduzione 2

2.1. Descrizione del DiskCrypt *Mobile* DCM300 2
2.2. DCM300 Porte di connessione 3
2.3. Contenuto della confezione 3
2.4. Specifiche tecniche 4

3. Installazione 5

3.1 Installazione dell' hard-disk 5
3.2 Connessione del DCM300 al computer via USB 6
3.3 Connessione del DCM300 al computer via Firewire 7
3.4 DCM300 a catena 8
3.5 Utilizzo della tastiera 9
3.6 Utilizzo dell'alimentatore 10

4 Autenticazione 11

4.1 Inserimento della smart card 11
4.2 Inserimento del PIN 11

5 Settaggio del Drive 12

5.1 Settaggio di un nuovo Drive 12
5.2 Settaggio di un Drive esistente 12

6 Disconnessione del DCM300 13

7 Caratteristiche di sicurezza delle Smart Card 14

7.1 Cambio del PIN 14
7.2 Modalità Amministrazione 15

8 Accessori opzionali 18

8.1 DigiSAFE DCM Management Software (DMS) 18

9 Informazioni utili 19

9.1 Partizionare e formattare il disco 19

10 Uso e manutenzione 20

11 FAQ – Domande frequenti 21

12 Problemi 24

AMENDMENT RECORD

AMDT NO.	AFFECTED PAGE(S)	ECN/DCR NO.	EFFECTIVE DATE

1. Informazioni sul manuale

Questo manuale di uso fornisce informazioni passo passo per l'installazione del DigiSAFE DiskCrypt *Mobile* DCM300 e per il suo utilizzo.

LEGGERE E SEGUIRE ATTENTAMENTE
LE ISTRUZIONI D'USO CONTENUTE
In mancanza di un utilizzo corretto si potrebbero
verificare danni al DiskCrypt Mobile o ai dispositivi
ad esso collegati.

2. Introduzione

2.1. Descrizione del DiskCrypt *Mobile* DCM300

Congratulazioni per l'acquisto di DigiSAFE DiskCrypt *Mobile* DCM300. DiskCrypt *Mobile* DCM300 rappresenta il sistema di memorizzazione mobile più avanzato oggi disponibile, che utilizza autenticazione con smart card e crittazione dell'intero disco con AES 128/256 bit. Con DiskCrypt *Mobile*, puoi avere un sistema di memorizzazione conveniente e rapido, compatibile con USB 2.0 e Firewire 400/800, estremamente compatto e che protegge in modo efficace tutti i tuoi dati da occhi indiscreti.

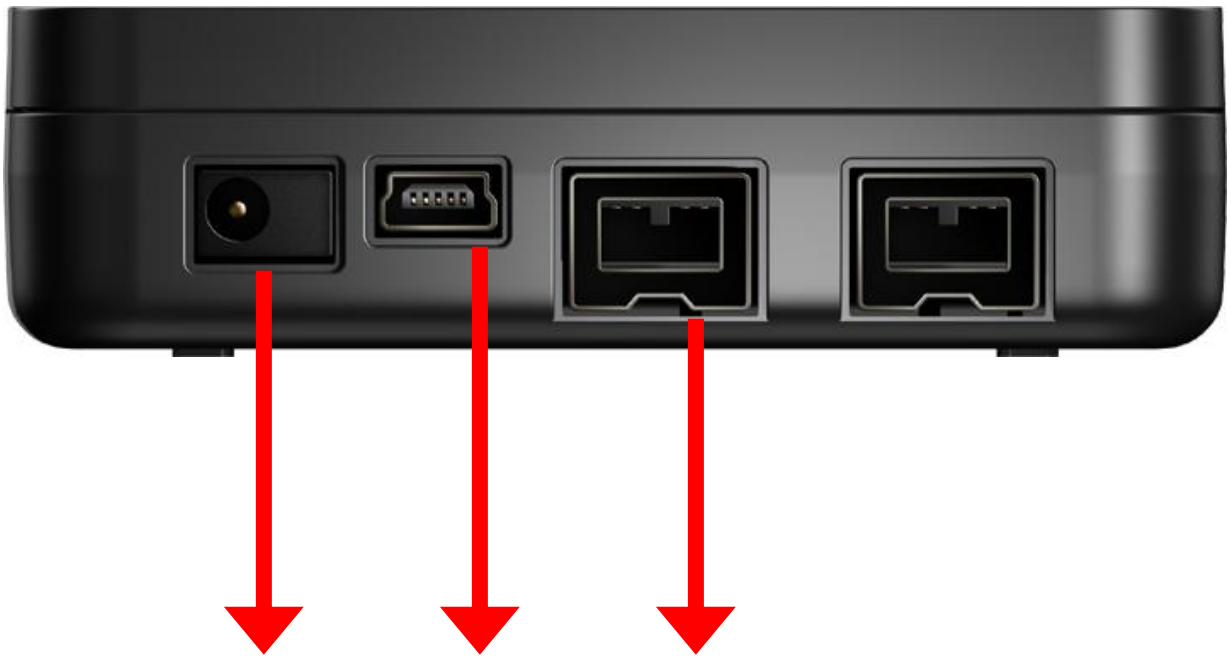
DCM300 è un box portatile e sicuro per hard-disk SATA da 2.5" e un modulo di crittazione hardware che agisce su ogni settore dell'hard-disk.
Cripta ogni singolo settore e ogni singolo byte che viene scritto nel disco.
E' progettato per l'utilizzo con hard-disk standard da 2.5" con interfaccia SATA, e e si collega al computer sia tramite porte standard USB 2.0 sia Firewire 400/800
Criptando ogni singolo byte e settore, DCM300 è indipendente dal sistema operativo e non necessita di alcun driver software. Cripta anche sia ogni singolo file temporaneo sia ogni area che i normali Software di crittazione lascerebbero invece "in chiaro".
crittazione e decrittazione avvengo in tempo reale senza nessuna degradazione delle performance del disco. L'Utente può semplicemente usare i suoi computer con la completa sicurezza che tutti i suoi dati saranno efficacemente protetti nello sfortunato caso in cui l'hard-disk venga perso o rubato.

DCM300 salva la chiave di crittazione nelle smartcard (2 in ogni confezione).
La tecnologia Smart card technology è di facile comprensione e rappresenta il più alto livello di sicurezza per la memorizzazione dei dati. E' molto più sicura delle altre tecnologie basate su Token, dove la chiave di crittazione viene memorizzata in chiavette USB facilmente duplicabili. Al contrario, le smartcard contengono la chiave in modo sicuro, e accessibile solo dopo la digitazione del codice PIN corretto. L'utente avrà bisogno sia della smartcard sia di conoscere il PIN corretto per poter accedere ai dati contenuti nell' hard-disk.

Grazie a questo sistema DCM300 sviluppa una autenticazione a due fattori che consente una Maggiore sicurezza, assicurando che solo un utente in possesso della smartcard e con la conoscenza del codice PIN corretto possa accedere ai dati.

All'utente viene richiesto di autenticarsi ogni volta che si collega il DCM300 al computer.
Solo dopo una corretta autenticazione il disco diventa visibile dal sistema operativo e l'utente può accedervi normalmente.

2.2. DCM300 Porte di connessione



2.3. Contenuto della confezione

I seguenti oggetti sono inclusi con DiskCrypt *Mobile* DCM300.
In caso di qualche mancaza si prega di contattare il vostro distributore/rivenditore.

- 1 x DigiSAFE DiskCrypt *Mobile* DCM300
- 1 x cavetto USB
- 2 x smart card DiskCrypt *Mobile*
- 1 x custodia nera

2.4. Specifiche tecniche

Dischi compatibili	• Dischi 2.5” SATA di ogni capacità (spessore max 9.5mm)
Interfaccia	• USB 2.0 • Firewire 400/800
Physical	• Connettore SATA 22 pin • Connessione USB mini-B • Connessione Firewire 9-pin • 1.3mm 5VDC jack • Slot Smart Card • Dimensioni: 130mm x 78mm x 22mm
Alimentazione	• Circa 5V 400mA max (escludendo la potenza necessaria per l'hard disk)
Autenticazione	• Autenticazione a 2 fattori con smart card e PIN
Smart Card	• Card supportate ISO-7816 T=0 Class B
Encryption	• Motore di crittazione hardware AES certificato NIST [1] • Chiavi supportate: 128bit/256bit
Gestione Chiavi	• PIN configurabile dall'utente • Password per modalità amministrativa
Certificazioni e Standard	• FIPS 140-2 Level 2FCC, CE • FCC, CE • RoHS
Sistemi Operativi	• Indipendente dal sistema operativo • Testato con Windows® Seven, XP, 2000, Mac OS X e Linux

[1] NIST – The National Institute of Standards and Technology of the United States of America

3. Installazione

Per utilizzare DiskCrypt *Mobile* DCM300 rimuovere delicatamente la parte superiore del box e installare il proprio hard-disk SATA da 2.5" connettendolo saldamente all'apposito connettore a 22pn.
In questa sezione troverete istruzioni più dettagliate step-by-step.

Se la tua unità ha un hard disk preinstallato, puoi saltare questa sezione e passare direttamente alla sezione 3.2.

3.1 Installazione dell' hard-disk

DiskCrypt *Mobile* DCM300 supporta hard-disk standard SATA 2.5" di ogni capacità.
Per l'installazione seguire i seguenti passaggi:

1. Aprire il DCM300 e rimuovere delicatamente la copertura superiore premendo l'apposito pulsante che si trova su un lato dell'unità.

2. Connettere saldamente l'hard disk SATA da 2,5" all'apposito connettore da 22 pin che si trova da un lato.

3. Riposizionare attentamente la copertura superiore.

Note:
- *Assicurarsi che la copertura superiore sia saldamente posizionata.*

3.2 Connessione del DCM300 al computer via USB

Dopo aver correttamente installato l'hard-disk nel DCM300, è possibile procedere con la connessione al computer.
Seguire i seguenti passaggi:

1. Inserire il cavo USB nella porta corrispondente del computer.

2. Inserire il cavo USB tipo B nella porta del DCM300. Assicurarsi che l'orientamento del cavo sia corretto.

3. Gli indicatori ACTIVE, STATUS e ERROR si illumineranno in sequenza (vedere la Sezione 3.5 su Utilizzo della tastiera per localizzare i LED). In seguito, la retroilluminazione del DCM300 si accenderà indicando che l'alimentazione è avvenuta correttamente.

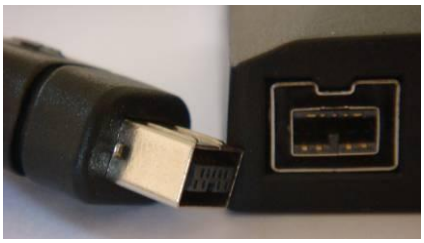
Note sull'uso con porte USB:

- *Non collegare il DCM300 ad hub USB esterni o a prolunghe USB.*
- *Connessioni a porte non standard USB possono causare danneggiamenti o errori.*
- *Se l'alimentazione risulta insufficiente, connettere entrambi i connettori del cavo USB alle porte del computer.*
- *Per sfruttare la velocità dell'USB 2.0 connetere sempre a porte USB 2.0 Hi-Speed.*

3.3 Connessione del DCM300 al computer via Firewire

Per connettere il DCM300 al computer via Firewire, seguire i seguenti passaggi:

1. Inserire il connettore Firewire nella porta del Firewire del computer. Se il computer supporta Firewire 800 con porta a 9 pin, sarà necessario un cavo Firewire a 9 pin da entrambi i lati. Connettere semplicemente il cavo alla porta Firewire del computer.



2. Inserire il connettore Firewire a una delle 2 porte Firewire del DCM300. Assicurarsi che il connettore sia orientato correttamente.

3. Gli indicatori ACTIVE, STATUS e ERROR si illumineranno in sequenza (vedere la Sezione 3.5 su Utilizzo della tastiera per localizzare i LED). In seguito, la retroilluminazione del DCM300 si accenderà indicando che l'alimentazione è avvenuta correttamente.

***Note sull'uso delle porte Firewire**:*

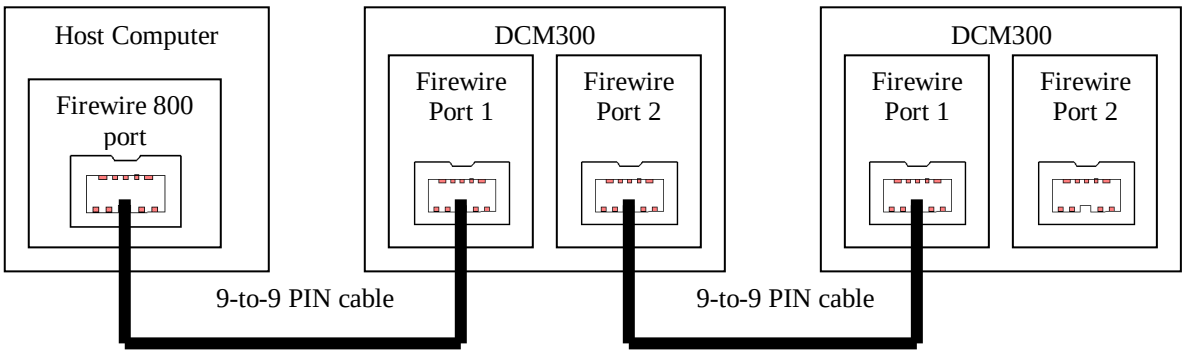
- *Il cavo Firewire non è incluso nella confezione.*
- *Se la connessione Firewire non fornisce sufficiente alimentazione, sarà necessario l'uso di alimentatore esterno. Per favore riferirsi alla Sezione 3.6 su* Utilizzo dell'alimentatore*.*
- *Se il computer supporta Firewire 400 con porta a 6 pin, asicurarsi di avere un cavo a 9 pin da un lato e 6 dall'altro. Connettere il connettore a 6 pin al computer, e quello a 9 pin al DCM300.*

- *Se si utilizza Firewire 400 e un cavo a 9 pin da un lato e 4 dall'altro, sarà necessario utilizzare un alimentatore esterno per il DCM300. Per favore riferirsi alla Sezione 3.6 su* Utilizzo dell'alimentatore*.*

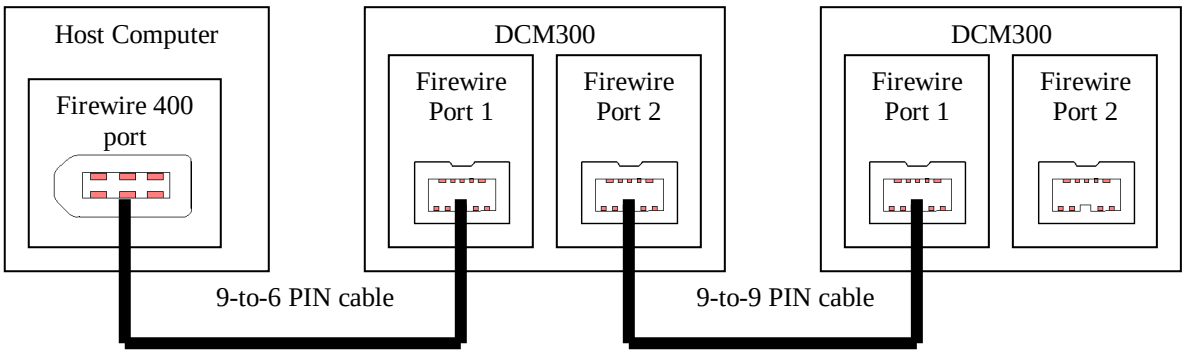
3.4 DCM300 a catena

Ogni DCM300 disponedi due porte Firewire per permettere il collegamento a catena di due o più DCM300 e/o altri hard-disk Firewire. Per l'utilizzo a catena riferirsi alla seguenti configurazioni:

Configurazione 1: Connessione a un computer che supporta Firewire 800



Configurazione 2: Connessione a un computer che supporta Firewire 400



3.5 Utilizzo della tastiera

La tastiera integrata permette di inserire/cambiare il proprio PIN (rif. Sez. 4 per *Autenticazione* e rif. Sez. 7 per *Modificare il PIN).* Funziona semplicemente premendo delicatamente i numeri o le scritte desiderati.

Note:

- *NON utilizzare forza eccessiva premendo sulla tastiera.*
- *Utilizzare una pressione eccessiva può portare nel tempo ad una diminuzione della sensibilità dei tasti.*

Indicatori LED di stato

3.6 Utilizzo dell'alimentatore

DCM300 è progettato per essere alimentato tramite USB. Tuttavia, in alcuni computer, l'alimentazione tramite bus USB potrebbe risultare insufficiente. In questi casi è Necessario un alimentatore esterno.

Specifiche tecniche per l'alimentatore:
Input: 100-240V AC, 50-60Hz, 0.5A
Output: +5V DC, 2A
DC connettore: 1.3mm

***Note**:*

- *L'alimentatore non è incluso nella confezione.*
- *Assicurarsi di utilizzare un alimentatore corretto. L'utilizzo di un alimentatore scorretto potrebbe causare malfunzionamenti e danni.*
- *DCM300 resta in modalità autenticata finchè alimentato. Assicurarsi di scollegarlo quando ci si allontana.*

4 Autenticazione

DCM300 richiede l'autenticazione a due fattori prima di garantire l'accesso al disco.
Per farlo bisogna utilizzare la smartcard e il PIN associati.
Il processo di autenticazione richiede l'inserimento della smartcard nel DCM300 seguito dal PIN corretto. Una volta completato correttamente il processo, il disco apparirà al sistema operativo e potrà essere utilizzato liberamente.

4.1 Inserimento della smart card

DCM300 viene fornito con 2 smart card. DigiSafe raccomanda di usare una sola card e tenere la seconda in un posto sicuro. Così nell'eventualità che la prima card venga persa o rubata, si potrà usare quella rimanente per l'autenticazione.

Per iniziare l'autenticazione, inserire semplicemente la smart card con i contatti verso il basso. La card può essere inserita prima o dopo il collegamento al PC. Una volta inserita la card corretta, i LED di stato lampeggeranno. Se verrà inserita una card scorretta lampeggerà il LED di errore.

4.2 Inserimento del PIN

Una volta inserita una card corretta, si potrà procedere con la digitazione del PIN ad 8 Caratteri. Il PIN di default è **12345678**. Dopo aver inserito il PIN premere il tasto **ENTER**.

***Note**:*

- *In caso venga inserito un PIN scorretto il LED **Error** lampeggerà in modo continuato. Premere **ESC** per resettare il DCM300. Per correggere l'inserimento di un PIN errato premere sempre **ESC**.*

- ***Dopo 8 tentativi** di utilizzare un PIN errato, verrà bloccato l'accesso alla smartcard. Si consiglia quindi di contattare l'assistenza tecnica dopo circa 5 tentativi scorretti, come mostrato nella sezione 11. Problemi.*

Inserire la smart card con i contatti rivolti verso il basso e con la scrittaDigisafe rivolta verso l'alto.

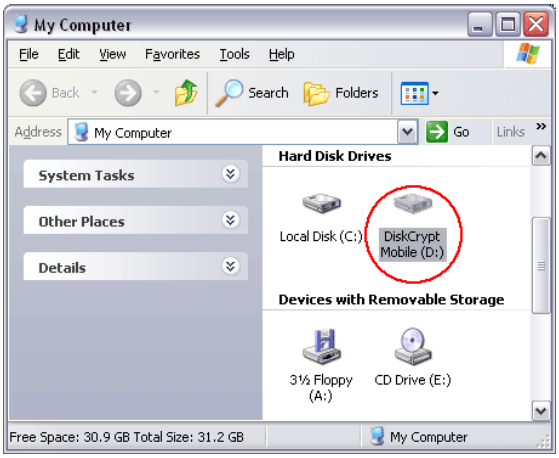
*Digitare il PIN di 8 cifre e poi premere il tasto **ENTER***

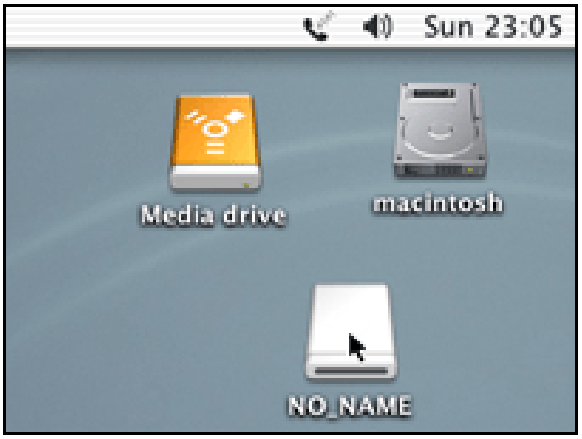
5 Settaggio del Drive

Dopo una corretta autenticazione col DCM300, l'accesso al disco sarà garantito.
Il Drive sarà visibile dal sistema operativo come un normale disco removibile.
Il processo di riconoscimento durerà qualche secondo, in base al disco e al sistema operativo.

In caso di installazione di un hard disk nuovo comprato da un rivenditore, sarà necessario inizializzare e formattare il drive (vedere la sezione 5.1). In caso contrario, procedure all'accesso al disco second la normale procedura (vedere la sezione 5.2).

Una volta che il disco sarà stato riconosciuto si potrà usarlo esattamente come un normale disco removibile.





5.1 Settaggio di un nuovo Drive

Per utilizzare un hard-disk nuovo è necessario effettuare partizionamento e formattazione. Per questi passaggi seguire le istruzioni del proprio sistema operativo o consultare la sezione *9.1 Partizionare e formattare il disco*.

5.2 Settaggio di un Drive esistente

Nessuna operazione addizionale richiesta per preparare un drive già formattato.
Una volta che il Drive sarà riconosciuto dal sistema operativo, si potrà procedere con il normale utilizzo.

Note:

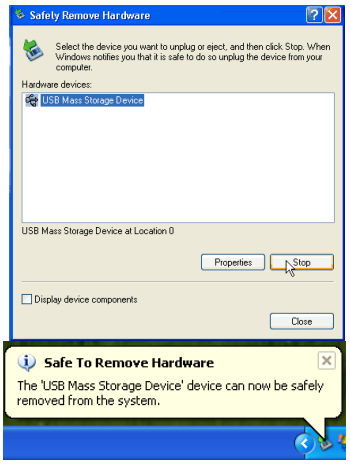
- *Quando si utilizza un disco preformattato, assicurarsi che il file system sia compatibile con il proprio sistema operativo.*
- *DCM300 fornisce protezione sui dati restanti. Dopo una corretta autenticazione, il disco potrà essere utilizzato normalmente. Per la massima sicurezza, non lasciare incustodito il DCM300 in modalità autenticata quando ci si allontana dal PC.*
- *Come con tutti i drive esterni si consiglia di effettuare backup regolari per evitare possibili perdite di dati.*

6 Disconnessione del DCM300

ATTENZIONE: per evitare perdite di dati, assicurarsi di chiudere tutte le applicazioni attive prime di disattivare il DCM300.

Per disconnettere il DCM300 seguire i passaggi in base al sistema operativo.

Windows XP


Safely Remove Hardware
Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.
Hardware devices:
USB Mass Storage Device
USB Mass Storage Device at Location 0
Properties
Stop
Display device components
Close
Safe To Remove Hardware
The 'USB Mass Storage Device' device can now be safely removed from the system.

1. Doppio click su **Rimozione sicura hardware**.
2. Selezionare **Dispositivo di archiviazione USB**, e selezionare il dispositivo da rimuovere.
3. Clicare **Scollega.**.
4. Cliccare **OK** per confermare la disconnessione.
5. Cliccare **Chiudi**.
6. Windows informerà che il disco può essere rimosso in sicurezza.
7. Ora il DCM300 può essere disconnesso in modo sicuro dal pc.

Mac

1. Trovare l'icona **Disco removibile** associata al DCM300.
2. Trascinare l'icona nel **Cestino** e aspettare che scompaia.
3. Ora il DCM300 può essere scollegato in modo dal computer.

7 Caratteristiche di sicurezza delle Smart Card

Con DCM300 si possono utilizzare alcune funzioni relative alla sicurezza tipiche delle Smart card. Queste funzioni sono utilizzabili solo in fase di autenticazione.
Sono disponibili le seguenti funzioni.

ATTENZIONE: le funzioni di sicurezza/amministrazione delle smart card devono essere esguite con molta cautela in quanto causano cambiamenti nelle card e nei PIN associati. Si prega di leggere le seguenti istruzioni attentamente e di seguirle scrupolosamente utilizzando funzioni amministrative.

7.1 Cambio del PIN

Con DCM300 si può cambiare il PIN associato alla propria smart card. Si raccomanda di cambiare il PIN di default e di usarne uno nuovo segreto.
Per cambiarlo seguire i seguenti passaggi:

1. Inserire la smart card nel DCM300.
2. Premere il pulsante **Change PIN**, seguito dal tasto "**1**".
3. Premere **Enter**. Il LED Status lampeggerà 3 volte.
4. Digitare il PIN corrente e premere **Enter**. Il LED Status lampeggerà 2 volte per notificare di inserire il nuovo PIN.
5. Digitare il nuovo PIN e premere **Enter**. Il LED Status lampeggerà 2 volte per segnalare che si dovrà digitare il nuovo PIN per conferma.
6. Digitare il nuovo PIN e premere **Enter**.

Una volta cambiato correttamente il PIN, il DCM300 procederà a connettere il drive.
Allo stesso tempo il LED Status lampeggerà 3 volte e saranno emessi 2 "*beep*".
In caso contrario il LED Error lampeggerà in modo continuato.

***Note**:*

- *DCM300 accetta solo PIN di 8 cifre. Se viene inserito un PIN più corto o più lungo, il LED Error lampeggerà. Premere il tasto **ESC** per ricominciare il processo di autenticazione. Si dovrà riprendere il processo dal passaggio 2.*
- *Premere il tasto **ESC** farà ripartire il processo di autenticazione.*
- *Ogni smart card ha un proprio PIN associato. Si prega di notare che si possono utilizzare PIN differenti per ognuna delle 2 smart card incluse col DCM300.*
- ***Inserendo 8 volte un PIN scorreto la smart card verrà bloccata.***

7.2 Modalità Amministrazione

Si può accedere al DCM300 in modalità amministrazione. In questo modo si potrà cambiare il PIN amministrativo e/o inizializzare le Smart card per utilizzarle con il DCM300.
Smart card addizionali possono essere acquistate separatamente. Sarà necessario utilizzare Smart card supportate da DigiSafe e conoscere il PIN amministrativo.
Il PIN amministrativo di default è "**87654321**".
Per uscire dalla modalità amministrativa ricollegare il cavo USB.

7.2.1 Inizializzazione Smart Card

Per inizializzare una smart card seguire i seguenti passaggi:

1. Inserire una nuova smart card nel DCM300.
2. Il LED Error si illuminerà segnalando che è stata inserita una card non valida. Ignorare il LED.
3. Premere il tasto **Admin** seguito da **Enter**. Il LED Status lampeggerà 3 volte.
4. Digitare il PIN amministrativo e premere **Enter**. Il LED Status lampeggerà 3 volte e, se il codice inserito è corretto, si sentiranno 2 "*beep*".
5. DCM300 procederà con l'inizializzazione della smart card in modo che sia utilizzabile con quel particolare DCM300.
6. Rimuovere e riconnettere il cavo USB per uscire dalla modalità amministrazione.

***Note**:*

- *Una volta inizializzata una nuova smart card, si dovrà ripartizionare/formattare il disco esistente poiché la chiave di crittazione sarà differente.* ***Tutti i dati esistenti saranno illeggibili con la nuova smart card**.*

- *NON è possible connettersi all' hard disk in modalità amministrazione. Per farlo, rimuovere e riconnettere il cavo USB per uscire dalla modalità amministrazione, quindi inserire il PIN della smart card per autenticarsi al DCM300.*

7.2.2 Modalità di blocco delle Smart Card (SOLO DCM300-256bit da 07/2011)

DCM300 permette all'utente di scegliere due modalità di blocco delle smart card. Questo controlla il modo in cui il DCM300 si comporta quando viene rimossa la smart card dopo l'autenticazione. Sono supportate due modalità:

1. Nessun blocco – DCM300 rimane connesso anche se si disinserisce la smart card. Il LED di status è **verde** in modalità autenticata.
2. Blocco – DCM300 si disconnette automaticamente se disinserita la smart card. Il LED di status è **rosso** in modalità autenticata.

Per passare da una modalità di blocco ad un altra, seguire i seguenti passaggi:

1. Inserire la smart card nel DCM300.
2. Premere **Admin**, seguito dal tasto '1'.
3. Premere **Enter**. Il LED di Status lampeggerà 3 volte.
4. Inserire il PIN di amministrazione (8 cifre) e premere **Enter**. Il LED di status lampeggerà 3 volte e si sentiranno 2 'beep' se è stato inserito il PIN corretto.
5. DCM300 cambierà la modalità di blocco. Controllare il colore del LED di status per capire la modalità di blocco attivata.
6. Rimuovere e riconnettere il cavo USB per uscire dalla modalità di amministrazione.

***Note**:*
- *La modalità di default è "Nessun blocco".*
- *In modalità "Blocco", DCM300 si disconnette automaticamente una volta disinserita la smart card. **NON** rimuovere la smart card durante l'accesso al DCM300 in quanto potrebbe causare la perdita o il danneggiamento irreversibile dei dati al suo interno.*

7.2.3 Cambiare PIN amministrativo

Il PIN amministrativo fornisce ulteriore protezione per evitare che utenti non autorizzati possano utilizzare il DCM300 senza autorizzazione. Si raccomanda di cambiare il PIN amministrativo di default e utilizzarne uno segreto. Per cambiarlo procedere con i seguenti passaggi:

1. Inserire la smart card nel DCM300.
2. Premere il tasto **Change Pin**, seguito dal tasto **'0'**.
3. Premere **Enter**. Il LED Status lampeggerà 3 volte.
4. Digitare il PIN amministrativo e premere **Enter**. Il LED Status lampeggerà 2 volte per segnalare che si potrà inserire il **nuovo** PIN amministrativo.
5. Digitare il **nuovo PIN** e premere **Enter**. Il LED Status lampeggerà 2 volte per segnalare di inserire nuovamente il **nuovo PIN** per conferma.
6. Digitare il **nuovo PIN** e premere **Enter**.
7. Il LED Status lampeggerà 3 volte seguito da 2 "*beep*" per segnalare che il cambio è PIN avvenuto correttamente.
8. Rimuovere e riconnettere il cavo USB per uscire dalla modalità amministrazione.

In caso venga digitato un PIN errato, premere il tasto **Esc** in qualunque momento per far ripartire il processo dall'inizio.

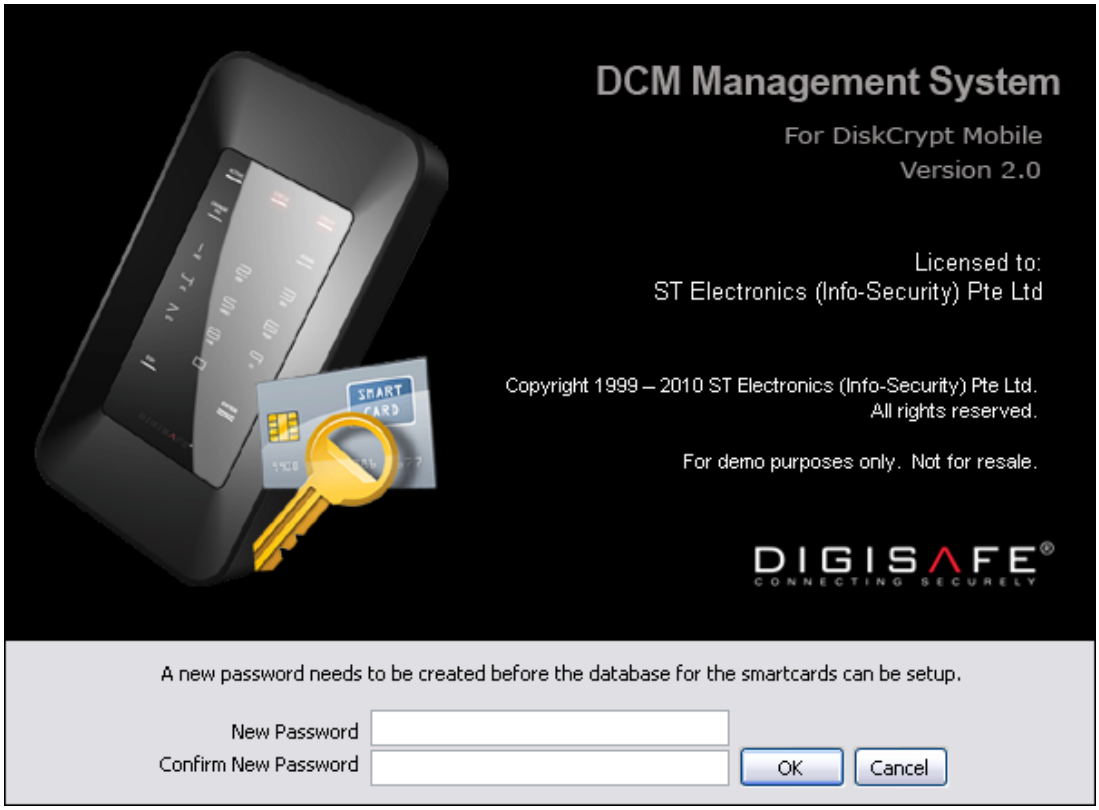
***Note**:*

- *Come il PIN per le smart card, così anche il DCM300 accetta solo codici PIN di 8 cifre. Se viene inserito un PIN più corto o più lungo, il led Error lampeggerà continuamente. Premere il tasto **Esc** per ricominciare il processo di autenticazione. Sarà necessario ricominciare la procedura dal passaggio 2.*

8 Accessori opzionali

8.1 DigiSAFE DCM Management Software (DMS)

DigiSAFE DCM Management Software (DMS) fornisce la possibilità di gestire le proprie smart card per l'uso con il DCM300. Gli amministratori di sistema possono anche usare questo software per fare il back up delle chiavi di crittografia che vengono precaricate nelle smart card fornite con il DCM300.


DCM Management System
For DiskCrypt Mobile
Version 2.0
Licensed to:
ST Electronics (Info-Security) Pte Ltd
Copyright 1999 – 2010 ST Electronics (Info-Security) Pte Ltd.
All rights reserved.
For demo purposes only. Not for resale.
DIGISAFE
CONNECTING SECURELY
A new password needs to be created before the database for the smartcards can be setup.
New Password
Confirm New Password
OK
Cancel

DigiSAFE DMS permette le seguenti operazioni:

1) Cambio PIN delle smart card
2) Generazione e caricamento delle chiavi di crittografia in nuove smart card.
3) Duplicazione di smart card con la stessa chiave di crittografia
4) Editing dei record delle smart card
5) Lettura e back up delle chiavi di crittografia delle smart card
6) Eliminazione dei record dalle smart card

***Note**:*

- *Riferirsi al manual del DigiSAFE Smartcard Management per le istruzioni sul suo utilizzo.*
- *Contattare il proprio rivenditore per domande o per l'acquisto del software e/o di nuove smart card DigiSAFE.*

9 Informazioni utili

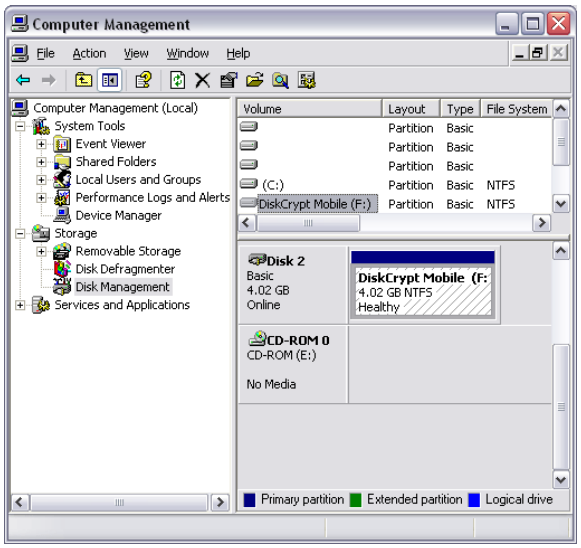
9.1 Partizionare e formattare il disco

Per utilizzare un disco nuovo con il DCM300, bisogna procedere con partizionamento e formattazione. Per procedere seguire i seguenti passaggi:

ATTENZIONE: le operazioni di partizionamento/formattazione cancellano tutti i dati presenti sul disco.

Windows XP

1. Connettere il DCM300 e autenticarsi.
2. Cliccare col tasto destro su **Risorse del Computer** e selezionare **Gestione.**
3. Da Gestione Computer selezionare **Gestione Disco.**
4. Cliccare col tasto destro sul Disco e selezionare **Inizializza**.
5. Cliccare col tasto destro sul disco e selezionare **Nuova Partizione**.
6. Seguire il Wizard per creare il numero di partizioni desiderate.
7. Cliccare col tasto destro sulle partizioni create e selezionare **Formatta**. Utilizzare FAT32 o NTFS.
8. Una volta completata la formattazione il drive sarà pronto per essere utilizzato.

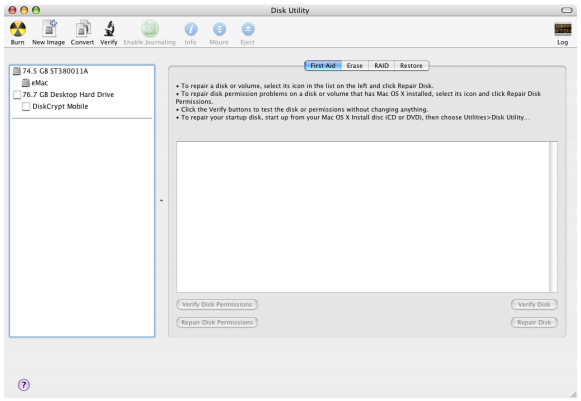


***Note**:*

- *Per utilizzare le utility di Gestione del disco è necessario utilizzare un account amministratori in windows.*
- *Per utilizzare dischi da più di 137GB è necessario Windows SP3 per windows 2000 e SP1 per Windows XP.*

Mac

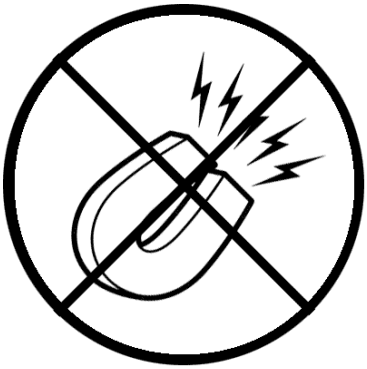
1. Connettere il DCM300 e autenticarsi.
2. Entrare in **Applicazioni** e poi in **Utilità**
3. Eseguire **Disk Utility**.
4. Selezionare DCM300 sulla colonna sinistra e cliccare su **Partiziona**.
5. Scegliere Numero, Dimensione e Nomi per le partizioni desiderate.
6. Mac OS formatterà il disco automaticamente
7. Una volta terminato il processo, il disco potrà essere utilizzato correttamente.



10 Uso e manutenzione

Di seguito alcune informazioni importanti su uso e manutenzione del DCM300.
Si prega di leggere le seguenti istruzioni:

- Come per ogni disco, si consiglia di creare regolarmente backup dei dati.
- Assicurarsi di seguire la corretta procedura per disconnettere il DCM300.
- Non muovere o disconnettere il DCM300 durante operazioni di scrittura/lettura per evitare malfunzionamenti o danneggiamenti dei dati.
- NON esporre il DCM300 a fonti di calore, fiamme o calore eccessivo.
- NON avvicinare ad apparecchiature che producono forti campi elettromagnetici. L'esposizione a tali campi potrebbe causare malfunzionamenti o danneggiamento dei dati.
- Evitare cadute o colpi al DCM300.
- Evitare contatti con acqua o altri liquidi.
- NON cercare di disassemblare o revisionare il DCM300.



11 FAQ – Domande frequenti

Cos'è DiskCrypt Mobile DCM300?

DiskCrypt *Mobile* DCM300 è un contenitore per hard-disk SATA da 2.5” con sistema di cifratura. Fornisce controllo di accesso con autenticazione a due fattori e sicurezza tramite la crittazione dell'intero disco.

DiskCrypt Mobile DCM300 è facilmente utilizzabile?

Il suo utilizzo è molto semplice e chiaro. Dopo l'installazione del disco nel DCM300, basta collegare il computer, inserire la smart card e digitare il PIN. Non è necessario installare alcun software.

Quali vantaggi offre DiskCrypt Mobile rispetto ad altri dischi USB portatili?

DiskCrypt *Mobile* fornisce il massimo della sicurezza tramite l'autenticazione a due fattori e la crittazione hardware dell'intero disco. E' l'unico hard disk portatile che utilizza le smart card per una doppia autenticazione.

Quali vantaggi offre l'autenticazione con Smart card rispetto ai normali prodotti come chiavi usb e token?

Le smart card sono una tecnologia provata per la sicurezza nella memorizzazione di informazioni.
DiskCrypt *Mobile* memorizza la chiave di cifratura all'interno della smart card. Al contrario altri dischi protetti, per salvare la chiave di cifratura, utilizzano chiavi usb che sono meno sicure e facilmente duplicabili se perse o rubate, compromettendo la protezione e la sicurezza dei dati nel
disco. Le smart card invece richiedono un PIN per l'accesso ai dati. Per cui anche in caso di smarrimento o furto delle card i dati nel disco rimarranno al sicuro poiché il PIN è conosciuto solo dal legittimo proprietario.

Cos'è l'autenticazione a 2 fattori?

L'autenticazione a due fattori è un protocollo di autenticazione che richiede due metodi Indipendenti per stabilire identità e permessi dell'utente. DiskCrypt *Mobile* implementa la doppia autenticazione richiedendo all'utente sia il possesso fisico della smart card corretta che la conoscenza
del PIN ad essa associato. Questo fornisce una sicurezza superiore rispetto ai normali sistemi di sicurezza basati su password e token.

Quali vantaggi fornisce l'autenticazione a 2 fattori?

L'autenticazione a 2 fattori fornisce una sicurezza superiore rispetto ai normali sistemi di sicurezza basati su password, token o sistemi biometrici. Anche se venissero sottratti sia il DCM300 sia la smart card, i dati sarebbero ancora sicuri grazie al PIN conosciuto solo dal legittimo proprietario.

Quali vantaggi offre la crittazione dell'intero disco rispetto alla protezione software?

Al contrario delle soluzioni software, DiskCrypt *Mobile* cripta ogni singolo byte e ogni singolo settore dell'hard disk. Questo significa che tutti i file temporanei, tutte le partizioni e anche tutti i settori di boot sono Criptati.
Il più grande svantaggio dei sistemi basati su crittazione software è che dipendono dal sistema operativo utilizzato, mentre DCM300 è indipendente dal sistema operativo.
DiskCrypt *Mobile* non richiede nessuna tediosa installazione o configurazione di software potenzialmente suscettibile di errore. Basta collegarlo al computer, autenticarsi correttamente ed è pronto all'uso.
DiskCrypt *Mobile* non richiede nessuna manutenzione *o* aggiornamento riducendo a zero i costi.
Non avviene nessuna degradazione delle performance del disco a causa della crittazione/decrittazione dei dati,al contrario delle soluzioni basate su software.

Cosa accade in caso di guasto al DiskCrypt Mobile?

Ogni DiskCrypt *Mobile* è sottoposto a rigorosi test qualitativi prima della spedizione. Tuttavia, l'hard disk al suo interno ha una durata di vita limitata. Per questo si consiglia di fare back up regolari di tutto il contenuto del disco. La chiave di crittazione è conservata all'interno della smart card, quindi anche in caso di malfunzionamenti del DiskCrypt *Mobile, i dati* resteranno leggibili fino a che si possiederà la smart card. Semplicemente basterà installare il disco all'interno di un altro DiskCrypt *Mobile* con la **stessa** crittazione (128 o 256 bit), inizializzare la smart card e si potrà ricominciare ad usare il DiskCrypt *Mobile* come al solito.

Viene protetto anche il settore di boot?

Si, DiskCrypt *Mobile* formisco full disk encryption (FDE), il che significa che ogni singolo byte e Ogni singolo settore del disco vengono criptati.

La crittazione incide sulle performance del disco?

No. Il motore di crittazione hardware on-the-fly del DiskCrypt *Mobile* DCM300 è più veloce dell'interfaccia di trasferimento dei dati SATA, per questo non ci sono degradazioni nelle Performance e non è richiesta nessuna ulteriore risorsa alla CPU.

Quanto è forte la crittazione di DiskCrypt Mobile?

DiskCrypt *Mobile* DCM300 offre uno schema di crittazione AES con lunghezza della chiave da 128bit o da 256bit.

Il PIN della smart card può essere cambiato senza perdita dei dati?

Si. Il PIN della smart card può essere facilmente cambiato durante la fase di autenticazione senza nessuna perdita dei dati. Si prega di notare che il PIN è specifico per ogni smart card quindi cambiando il PIN di una card non si cambia automaticamente anche quello dell'altra.

Posso usare DiskCrypt Mobile con il mio sistema operativo?

Si! DiskCrypt *Mobile* usa il proprio processore hardware per autenticazione e crittazione ed è indipendente dal sistema operativo. Basta utilizzare sistemi operativi che supportino le specifiche standard USB o quelle Firewire e si potrà utilizzare il DiskCrypt *Mobile.*
DiskCript *Mobile* è stato testato con Windows XP, 2000, Vista e Seven, Mac OS e anche Linux.

Cosa succede se si perde la smart card?

Le smart card incluse contengono la chiave di crittazione del disco installato. La chiave è protetta dal PIN, in modo sicuro fintanto che il PIN viene mantenuto segreto.
In caso di smarrimento della prima smart card, si può continuare ad accedere al disco grazie alla seconda card. In questo caso si consiglia di acquistare un nuovo set di smart card o il nostro sistema di gestione delle chiavi per duplicare le card. Si prega di notare che le nuove smart card utilizzano nuove chiavi di crittazione , per questo si consiglia di creare un back up dei dati esistenti prima di utilizzare le nuove card.

12 Problemi

In caso che il DCM300 non funzioni correttamente, si prega di riferirsi alla seguente lista per Scoprire il problema. Se è richiesto un ulteriore supporto tecnico, si prega di contattare il proprio rivenditore o il supporto tecnico DigiSAFE a:

STEE-InfoSec Technical Support
Email: services@digisafe.com

Problem	Query	Possible reason and remedy
La tastiera non è attiva	*La retroilluminazione dell'unità è accesa?*	Assicurarsi che il cavo USB sia saldamente collegato alla porta del computer. Se si usa la connessione Firewire, assicurarsi che il collegamento sia stato effettuato correttamente e saldamente.
	È stata inserita la Smart card?	Inserire la smart card correttamente Nel DCM300.
	Il LED Error è acceso?	Assicurarsi di aver inserito la smart card corretta, inserendola con il chip rivolto verso il basso.
Autenticazione	*Il LED Error è acceso?*	Assicurarsi di aver inserito la smart card corretta, inserendola con il chip rivolto verso il basso.
	Il LED Error è lampeggiante?	È stata inserita una password errata. Premere il tasto ESC e ricominciare il processo di autenticazione.
Il disco non è riconosciuto	*Il LED Status rimane acceso?*	Assicurarsi che il cavo USB sia saldamente collegato alla porta del computer. Se si usa la connessione Firewire, assicurarsi che il collegamento sia stato effettuato correttamente e saldamente.
	Sul computer appare l'icona del disco?	Controllare la presenza dell'icona nel sistema operativo. Assicurarsi che il DCM300 non sia collegato ad un HUB o una prolunga ma direttamente al PC. Se anche questo non basta, potrebbe essere necessario un alimentatore extra.
	Il disco è nuovo?	Per i nuovi dischi è necessario procedere con partizionamento e formattazione. Riferirsi al capitolo 8.1 Partizionamento e formattazione del vostro hard disk per ulteriori informazioni.

Problem	Query	Possible reason and remedy
Il disco non è riconosciuto	*Il File System è supportato dal sistema operativo?*	Quando si utilizza un disco esistente in un nuovo sistema operativo, assicurarsi che il file system del disco sia compatibilecol nuovo sistema operativo.
	DiskCrypt Mobile DCM300 è connesso ad una porta USB o Firewire?	Assicurarsi che il DCM300 sia collegato direttamente alla porta USB del PC e non tramite HUB o prolunghe. Se il disco non viene riconosciuto quando connesso alle porte frontale, provare con le posteriori. Se si utilizza il Firewire, provare ad utilizzare una porta Firewire differente sul computer host.
	Si sta utilizzando il cavo fornito in dotazione?	Usare solo il cavo fornito in dotazione col DiskCrypt Mobile certificato USB2.0 Y. Altri cavi potrebbe essere di bassa qualità.
	Dal drive provengono rumori intermittenti "click"?	Il disco potrebbe non ricevere sufficiente alimentazione dalla porta USB. Connettere entrambi i connettori direttamente nelle porte USB del PC e non tramite HUB o prolunghe. Se anche questo non basta, potrebbe essere necessario un alimentatore extra. Se si utilizza il Firewire, potrebbe essere necessario l'uso di un alimentatore esterno.
Il disco ha performance scarse	*DiskCrypt Mobile DCM300 è connesso ad una porta USB2.0?*	Per ottenere le performance USB2.0 Hi-Speed, assicurarsi che il DCM300 sia connesso ad una porta USB2.0.
	Si sta utilizzando il cavo fornito in dotazione?	Usare solo il cavo fornito in dotazione col DiskCrypt Mobile certificato USB2.0 Y. Altri cavi potrebbe essere di bassa qualità.
	DiskCrypt Mobile è connesso ad un HUB USB?	Connettere il DCM300 direttamente a due porte USB2.0 del computer.
	Altri dispositivi USB sono connessi alla stessa porta?	Scollegare gli altri dispositivi e controllare se le performance migliorano.